

REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks.

By this amendment, claims 1 and 12 are amended. No new matter has been added. Accordingly, claims 1-10 and 12-19 are pending in the present application.

Claim Rejections Under 35 U.S.C. § 101

Claims 1-10 and 16-18 are rejected under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter.

Independent claim 1 is amended, for clarification, to recite a method of generating electronic keys d for a public-key cryptography method using an electronic device, the method comprising, *inter alia*,

Step A ...

2) storing the pairs or values thus obtained in a memory of a secure electronic object; and

Step B ...

calculating a key d to be used by the secure electronic object from the retrieved pair (p, q) that is determined to be suitable.

Accordingly, the method recited in claim 1 is at least tied to a particular machine, e.g., the secure electronic object. In view of the foregoing, it is respectfully requested that the rejection of claims 1-10 and 16-18 under 35 U.S.C. §101 be withdrawn.

Claim Rejection Under 35 U.S.C. § 102

Claims 1-5, 12, 13, 15, 16 and 19 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Hopkins et al. (U.S. Patent Application Publication No. 2005/0190912 A1, hereinafter "Hopkins"). The rejection is respectfully traversed.

According to known technique of the Rivest Shamir and Adleman (RSA) scheme, carrying out an RSA key calculation requires knowledge of the public exponent e and the length l of the key. Specifically, with an input data e and l , a pair of prime numbers p and q is generated to satisfy certain conditions.

In comparison, according to Applicants' exemplary embodiments, in a first part of a method of generating electronic keys d , pairs of prime numbers (p, q) or values representative of pairs of prime numbers are calculated independent of knowledge of a pair of values (e, l) in which e is the public exponent and l is the length of the key of the cryptography method. The calculated pairs of prime numbers (p, q) or values representative of pairs of prime numbers are then stored in a memory of a secure electronic object, e.g., a SIM card of a telephone.

In a second part of the Applicants' exemplary method, knowledge of the pair (e, l) is obtained, and a pair of prime numbers (p, q) is selected from the stored calculated pairs prime numbers (p, q) to satisfy certain conditions based on the pair (e, l) .

Claim 1 recites a method of generating electronic keys d for a public-key cryptography method using an electronic device, comprising the following two separate calculation steps:

Step A

- 1) calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of a pair of values (e, l) in which e is the

public exponent and L is the length of the key of the cryptography method,

2) storing the pairs or values thus obtained in a memory of a secure electronic object; and

Step B

obtaining values for e and L ;

retrieving a pair of prime numbers (p, q) , or a value representative of said pair of prime numbers, stored in step A;

verifying the following conditions for said pair of prime numbers:

(i) $p-1$ and $q-1$ are prime numbers with the obtained value for e and

(ii) $N=p*q$ is an integer of given length L ,

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieving another pair of prime numbers and repeating the verification until a retrieved pair is suitable; and

calculating a key d to be used by the secure electronic object from the retrieved pair (p, q) that is determined to be suitable.

Hopkins fails to disclose every feature of claim 1. Hopkins discloses pre-computing sets of cryptographic parameter of different types, each type being adapted for use by an associated type of cryptographic application. Fig. 6 of Hopkins illustrates a process of providing pre-computed cryptographic parameters of different types. Referring to step 122 in Fig. 6, and paragraphs 0124 and 0125 of Hopkins, it is disclosed that the types of sets of cryptographic parameters pre-computed include sets of parameters that are most commonly used in cryptographic applications, in which a modulus n has a length L of 1024 bits, and a public exponent has value $e=3$.

Referring to step 124 of Fig. 6 in Hopkins, the cryptographic parameters pre-computed in step 122 are stored in a memory unit. Continuing to step 126 of Fig. 6 in Hopkins, a request for a set of cryptographic parameters having specified characteristic for use in received. Paragraph 0129 of Hopkins provides that the specified characteristic includes a specified length L of a requested modulus N and a specified public exponent value e .

Referring to step 128 of Fig. 6 in Hopkins, one of the pre-computed sets of cryptographic parameters is determined to have the specified characteristic in the request.

Hopkins does not anticipate Applicants' claim 1 at least for the following reasons.

First, in Hopkins, the pre-computed cryptographic parameters are generated for different values of length L and public exponent e . As mentioned above, at least step 122 in Fig. 6 and paragraphs 0124 and 0125 of Hopkins disclose that values of length L and public exponent e are used to generate pre-computed cryptographic parameters, which are subsequently stored in a memory. In contrast, according to claim 1, pairs of prime numbers (p, q) or values representative of pairs of prime numbers that are stored in the memory of the electronic object are calculated independent of knowledge of a pair of values (e, l) , and are stored in a memory of the secure electronic object. Thus, in the context of claim 1, the values for p and q that are stored in the memory are generated in the abstract, without being associated with specific values for e and l that may be required for a particular application. As such, they can potentially be used to calculate a number of different keys. In contrast, each set of cryptographic parameters is generated for a specific combination of L and e . Consequently, Hopkins fails to disclose the above-recited features of claim 1.

Second, claim 1 specifically recites obtaining values for e and l and verifying the following conditions for a pair of the stored prime numbers stored in the memory:

- (i) $p-1$ and $q-1$ are prime numbers with the obtained value for e and
- (ii) $N=p*q$ is an integer of given length l .

To the extent that Hopkins discloses verification in this paragraph, it is in connection with the initial computation of a set of cryptographic parameters. This process occurs prior to storage of the set in memory. See the flowchart of Figure 6 in which the computation step 122 is before the storage step 124.

Thereafter, Hopkins merely discloses that a determination is made at step 128 whether one of the pre-computed sets of cryptographic parameters has the characteristics specified in a request. Therefore, Hopkins does not explicitly disclose obtaining values for e and l and verifying the conditions (i) and (ii) for a pair of the stored prime numbers stored in the memory, as described in claim 1.

In addition, Hopkins does not inherently obtaining values for e and l and verifying the conditions (i) and (ii) for a pair of the stored prime numbers stored in the memory, as described in claim 1. Hopkins discloses that the pre-computed sets of cryptographic parameters are generated and stored in association with different values of public exponent e and length l . Therefore, it is likely that the choice of a pre-computed set of cryptographic parameters is made based on the public exponent e and length L that is used to generate the pre-computed sets of cryptographic parameters. In that case, the system as disclosed in Hopkins would not need to additionally verify conditions (i) and (ii), as described in claim 1, for a pre-computed set of cryptographic parameters stored in the memory. For this reason, Hopkins does not inherently disclose verifying the above-mentioned conditions (i) and (ii) for a pre-computed set of cryptographic parameters that is stored in the memory after a request containing specified characteristic of a key is received.

In rejecting claim 1, the Office Action refers paragraph 0063 of Hopkins as allegedly disclosing the claimed step of verifying conditions (i) for a calculated and stored pair of prime numbers. Applicants respectfully disagree.

Moreover, paragraph 0063 of Hopkins merely describes a constraint used in selecting a key for a multi-prime cryptographic system, instead of a classic two-prime cryptographic system. Paragraph 0063, however, does not disclose that such constraint is verified, after values of public exponent e and length L are received, for a pair of prime number that is pre-computed or stored. Therefore, paragraph 0063 of Hopkins does not disclose the claimed Step B, which includes verifying the following condition for a pair of stored prime numbers: (i) $p-1$ and $q-1$ are prime numbers with an obtained value for e , as described in claim 1.

At least for the reasons above, claim 1 is patentable. Independent claims 12 and 19 are patentable at least because they include distinguishing features similar to those of claim 1. Claims 2-5, 13, 15 and 16 are patentable at least because of their dependency.

Claim Rejections Under 35 U.S.C. § 103

Claims 6, 8-10, 14, 17 and 18 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins as applied to claims 1, 3, 5 and 13, and further in view of Futa et al. (U.S. Patent No. 7,130,422 B2, hereinafter "Futa").

Futa discloses a method of generating a prime N after receiving an input of prime q , wherein N is larger than q . Futa does not remedy the above-mentioned deficiencies of Hopkins. Therefore, claims 6, 8-10, 14, 17 and 18 are patentable.

Claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins in view of Futa as applied to claim 1, and further in view of Matyas (U.S. Patent No. 4,736,423, hereinafter "Matyas").

Matyas relates to reducing the size of cryptographic keys for storage on magnetic strip cards. Matyas does not remedy the above-mentioned deficiencies of Hopkins and Futa. Therefore, claim 7 is patentable.

CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: May 5, 2010

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620